From: CyberScoop
To: lmartin@bakersfieldpd.us
Subject: The number of security deals is just getting absurd
Date: Thursday, June 6, 2019 9:39:15 AM

Warning: This email originated from outside the City of Bakersfield. Think before you click!

Image

THURSDAY

June 6, 2019

The mergers and acquisitions activity in security continues to accelerate. A former fed explains the challenge that can arise with working with the Department of Homeland Security. And big companies should take a look at the dark web, if they're not already. This is CyberScoop for Thursday, June 6.

THIS IS JUST GETTING SILLY: Cisco today announced its intent to acquire the French industrial control company Sentryo. That's one day after Elastic said it will spend $234 million to buy Endgame. Both deals went down amid a frenzied period of M&A and funding activity in the security industry. Just look at CrowdStrike, which upped its IPO share price to a valuation of $6.2 billion from $4.5 billion. Market analysts predicted as much to CyberScoop last year. Bill Crowell, a partner at the venture capital firm Alsop Louie Partners, predicted number of companies will reduce by half within five to seven years, as many existing firms are acquired by larger players, and others simply go out of business. “Cyberdefense is about having an integrated set of tools that work together to prevent attacks,” he said. “But the industry now has a thousand points of light and no illumination. It’s as if in the automotive industry, a spark plug company advertised itself as making the best transportation service in the world.” Jeff Stone had that story.

WE'LL DO IT LIVE: A top federal cybersecurity official said Wednesday the Department of Homeland Security often lacks a clear picture of state and local governments’ network security, even as foreign adversaries increase their attempts to disrupt all levels of the public sector. And while federal agencies are getting better at working with state and local authorities, they face an ongoing challenge of staying ahead of an evolving threat landscape. “We don’t have good visibility in the state and local dot-gov [domain],” Rick Driggers, the deputy assistant director for cybersecurity at DHS’s Cybersecurity and Infrastructure Agency, said at FedScoop’s FedTalks event in Washington. Driggers said one of the most immediate steps state and local governments can take is to enact more robust information sharing with federal cybersecurity authorities. StateScoop's Benjamin Freed has more from FedTalks.

DC CYBERTALKS IS BACK!

Presented by CyberScoop, DC CyberTalks is a TED-like conference dedicated to addressing cybersecurity priorities, trends, innovations and the unprecedented security challenges ahead. For one day, 1,000 of the most influential cyber leaders from tech and government will gather in Washington, DC, to hear the industry's brightest speakers discuss the most critical issues in cybersecurity. Register now!

ARE YOU AFRAID OF THE DARK? If a cybercriminal wants to cause trouble for a major corporation, tools for the job are widely available on dark net markets, according to researchers who spent three months analyzing their activity and interacting with sellers. The wares — including malware and leaked credentials — are specifically promoted for breaching companies on the Fortune 500 and the Financial Times Stock Exchange 100 Index, according to Mike McGuire, a senior lecturer in criminology at the University of Surrey, and Bromium. The financial sector was the target of most of the malware tools (34 percent) for sale on the forums, which typically were only accessible with the anonymity software Tor. E-commerce was next, with 20 percent, followed by health care (15 percent) and education (12 percent). Dark web vendors offered unauthorized access, often in the form of stolen usernames and passwords, to business networks in those industries, too. Jeff has the research out today.

BEC SCAMS THAT SCALE: The decade-long evolution of one Western African cybercriminal gang is a “microcosm” for how criminals scale their business email compromise (BEC) scams, according to new research from Agari. The so-called Scattered Canary group’s rise from a lone individual to dozens of operatives specializing in various aspects of fraud illustrates the enduring effectiveness of BEC scams, which rely on social engineering

rather than fancy malware. “Most West African cybercriminal groups we track are organized in a similar hierarchy to Scattered Canary,” Agari’s Crane Hassold, a former FBI analyst, told CyberScoop. “Much like a business, these groups grow over time as their profits increase.” Sean Lyngaas has the story.

DC CYBERTALKS IS BACK!

Presented by CyberScoop, DC CyberTalks is a TED-like conference dedicated to addressing cybersecurity priorities, trends, innovations and the unprecedented security challenges ahead. For one day, 1,000 of the most influential cyber leaders from tech and government will gather in Washington, DC, to hear the industry's brightest speakers discuss the most critical issues in cybersecurity. Register now!

DITCH THE BOOKS: Hands-on experience is a critical component of cybersecurity education, and cyber ranges, like the one the University of Maine at Augusta opened last month, give students valuable experience a cybersecurity professor told EdScoop's Betsy Foresman. The pipeline of cybersecurity talent has been unable to keep pace with the dramatic rise in cybercrime, leaving many IT security teams shorthanded. As of January 2019, the United States has struggled to fill almost 314,000 cybersecurity jobs. “I want my students, when they graduate, to go and fill those jobs and to do very well at them,” said Henry Felch, a professor of computer information systems at the University of Maine at Augusta. He added that hands-on practice is one of the best ways for students to strengthen their skill sets and get a competitive edge for when they enter the workforce.

HOLD THAT POSE: A school district in upstate New York that had planned on Monday to begin operating a recently-installed facial recognition system will now postpone testing at the request of state

officials concerned with student privacy. Lockport City School District, a K-12 district of eight schools with about 4,400 students, announced on its website last week that it had finished installing video cameras backed by facial recognition software called Aegis, which is sold by a Canadian firm called SN Technologies. The school cited dismay at the school shootings reported in recent years and a need for “preventative measures.” Colin Wood has more at EdScoop.

TWEET OF THE DAY

Image

Pronounced "Lawl-ware."

How about tossing your favorite website a follow on Twitter and a like on Facebook? Click those shiny social buttons below to get the best we have to offer across the social web.

To learn about CyberScoop advertising and sponsorship opportunities, drop us a note - we look forward to hearing from you!

This newsletter is produced by Scoop News Group.
Visit cyberscoop.com to read this newsletter on the web.

Scoop News Group 1150 18th Street NW Suite 850 Washington, DC
You received this email because you are subscribed to CyberScoop from Scoop News Group.
Update your email preferences to choose the types of emails you receive.
Unsubscribe from all future emails